IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA, Plaintiff, vs. DOMINIC DZWONCZYK, Defendant.	4:15CR3134 BRIEF IN OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS

INTRODUCTION

On May 6, 2016, Defendant filed a Motion to Suppress "all evidence obtained and stemming from the government's search of Defendant's computer through deployment of a "network investigative technique" in violation of Federal Rule of Criminal Procedure 41 and Title 28, United States Code, Section 636(a)." (Filing 37, p. 1). In support of said motion, the Defendant filed a Brief and Index of Exhibits relating to the government's search of computers that accessed a TOR website known as "Playpen," executed in the Eastern District of Virginia on February 20, 2015. Defendant also cites to two cases in which district courts in Massachusetts and Oklahoma have agreed with defendants' contentions. The United States respectfully submits that for the reasons set forth in this response, Defendant's Motion to Suppress should be denied.

FACTS

The facts in the above-captioned matter are not in major dispute. On February 20, 2015, agents of the FBI applied for a search warrant in the Eastern District of Virginia requesting to use a network investigative technique ("NIT") to investigate users and administrators of the website "Upf45jv3bziuctnl.onion", referred to in the affidavit or search warrant as the "Target Website". The website, commonly and hereinafter referred to as "Playpen" was a site designed and utilized for the receipt and distribution of child pornography. The administrators and users

of the Playpen website would regularly send and receive illegal child pornography via the website. The targets of the investigation were the administrators and users of the Playpen website. (Filing 40, p. 15, ¶6).

The Playpen website operated as a "hidden service on the TOR network". (Filing 40, p.15). The website operated "on an anonymity network available to internet users known as "The Onion Router" or "TOR" network". (Filing 40, p. 15, ¶7). "In order to access the TOR network, a user must install TOR software, either by downloading an add-on to the users web browser or by downloading the free 'TOR browser bundle' available at www.TORproject.org." Id. at p. 16, ¶7. "The TOR software is designed to protect a user's privacy while on the web by bouncing their communications around a distributed network of relay computers run by volunteers all over the world, thereby masking the user's actual IP address which could otherwise be used to identify a user. It prevents someone attempting to monitor an internet connection from learning what sites a user visits, prevents the sites the user visits from learning the users physical location, and it lets the user access sites which could otherwise be blocked." Id. at p. 16, ¶8. Due to the masking of the user's actual IP address, "traditional IP identification check techniques are not viable." Id.

The TOR network further makes it possible for users to hide locations while at the same time offering a number of services within the TOR network. These services can include "web publishing, forum/website hosting, or an instant messaging server." Id. at p. 16, ¶9. As was the case with the Playpen website, the TOR network allows entire websites to be set up as "hidden services". Id. As explained in the affidavit,

> "hidden services" like other websites, are hosted on computer services that communication through IP addresses and operate the same as regular public websites, with one critical exception. The IP address for the web server is hidden, and instead is replaced with a TOR-based web address which is a series of

> algorithm-generated characters such as "asdlk8fs9dflku7f" followed by the suffice ".onion". A user can only reach these "hidden services" if the user is using the TOR client and operating in the TOR network. And unlike an open internet website, it is not possible to determine through public look-ups, the IP address of a computer hosting a TOR "hidden service." Neither law enforcement nor users can therefore determine the location of the computer that hosts the website through those public look-ups.

Id. at p. 16-17, ¶9.

Individuals did not access the Playpen website as one would on a traditional web-based service. Because the Playpen website was a "TOR hidden service," the user could only access the site through the TOR network. As explained in the affidavit,

> Even after connecting the TOR network, however, a user must know the web address of the website in order to access the site. Moreover, TOR "hidden services" are not indexed like websites on the traditional internet. Accordingly, unlike the traditional internet, a user may not simply perform a Google search for the name of one of the websites on TOR to obtain and click on a link to the site. A user might obtain the web address directly from communicating with other users of the board, or from internet postings describing the sort of content available on the website, as well as the websites location. For example, there is a TOR "hidden service" page that is dedicated to pedophilia and child pornography. That "hidden service" contains a section with links to TOR "hidden services" that contain child pornography. The [Playpen] website is listed in that section.

(Filing 40, p. 17, ¶10).

Thus, it was extremely unlikely that a person would go to the Playpen website without knowing the purpose of the site.

Between September 16, 2014, and February 3, 2015, FBI agents in the District of Maryland connected to the internet via the TOR browser and accessed the Playpen website. (Filing 40, p. 18, ¶11). As described in the affidavit, the Playpen website "appeared to be a message board website whose primary purpose is the advertisement and distribution of child pornography." Id. The log-in and registration information contained on the website clearly evidenced a desire for anonymity and nondisclosure. (Filing 40, p. 18-20, ¶12-13). The forums

found on the website focus on the distribution and accessing of child pornography. Id. at p.20, ¶14. Agents were also able to review many of the forums which appear to depict child pornography and child erotica involving prepubescent females, males and toddlers. The affidavit contains descriptions of various postings within these forums. (Filing 40, p. 22-25, ¶18-25). In addition, the Playpen website maintained sub-forums which contained "the most egregious examples of child pornography and/or dedicated to retelling of real-world, hands-on sexual abuse of children." A listing of the sub-forums is set out in the affidavit for search warrant. (Filing 40, p. 25-26, ¶27).

In December, 2014, a foreign law enforcement agency advised the FBI that a particular IP address was associated with the Playpen website. (Filing 40, p. 26, ¶28). Based on that information, the FBI obtained a search warrant and seized the server of the Playpen website. The server did contain a copy of the Playpen website. The server was then moved to a government facility in the Eastern District of Virginia for further investigation. The suspected administrator of the website was apprehended and allowed the FBI to assume administrative control of the Playpen website. (Filing 40, p. 26-28, ¶28-30).

As part of the affidavit, agents indicated that they would continue to operate the Playpen website from the government controlled computer server located in the Eastern District of Virginia. During this limited period of time, "not to exceed 30 days", the website would be operated in order to "locate and identify the administrators and users of [the Playpen website] through the deployment of the network investigative technique" described in the affidavit. As agents noted, "such a tactic is necessary in order to locate and apprehend the Target Subjects who are engaging in the continued sexual abuse and exploitation of children, and to locate and rescue children from the imminent harm of ongoing abuse and exploitation." (Filing 40, p. 28,

¶30). Agents requested authority to use the NIT, deployed from the Target Website operating in the Eastern District of Virginia, "to investigate any user or administrator who logs into the Target Website by entering a username and password." Id. at p.29, ¶32. Agents described the use of the NIT in the affidavit,

> In the normal course of operation, websites send content to visitors. A user's computer downloads that content and uses it to display webpages on the user's computer. Under the NIT authorized by this warrant, the [Playpen website], which will be located in Newington, Virginia, in the Eastern District of Virginia, would augment that content with additional computer instructions. When a user's computer successfully downloads those instructions from the [Playpen website], located in the Eastern District of Virginia, the instructions, which comprise the NIT, are designed to cause the user's "activating" computer to transmit certain information to a computer controlled by or known to the government. That information is described with particularity on the warrant (in attachment B of this affidavit), and the warrant authorizes obtaining no other information. The NIT will not deny the user of the "activating" computer access to any data or functionality of the user's computer.

(Filing 40, p. 29, ¶33). The NIT reveals various types of information, including the "activating computers actual IP address, active operating system username, and the computer's Media Access Control ("MAC") address, in order to attempt to identify the user of the site. In addition, agents noted in the affidavit that,

> In the normal operation of the website, a user sends "request data" to the website in order to access that site. While the [Playpen website] operates at a government facility, such request data associated with a user's actions on the [Playpen website] will be collected. That data collection is not a function of the NIT. Such request data can be paired with data collected by the NIT, however, in order to attempt to identify a particular user and to determine that particular user's actions on the [Playpen website].

Id. at p. 31-32, ¶37.

The search warrant requested by the agents was approved by a magistrate judge in the Eastern District of Virginia on February 20, 2015. Between February 20, 2015, and March 4, 2015, the Playpen website was operated by agents of the FBI and NIT was deployed each time a

user or administrator logged in to the Playpen website by entering a username and password. (Government's Index of Evidence, Document 1, p. 24-25, ¶24). During the government's control of the Playpen website, a user with the username "RebeckaBecka" engaged in accessing the Playpen website. (Government's Index of Evidence, Document 1, p. 25-26, ¶25-26). Information obtained through law enforcement indicated that the user "RebeckaBecka" engaged in activity on the Playpen website using the IP address 68.226.50.32. During the sessions, the user accessed images of child pornography through the Playpen website. (Government's Index of Evidence, Document 1, p. 26-27, ¶27-31). Further investigation determined that the IP address associated with the user "RebeckaBecka" was assigned to Cox Communications, an internet service provider serving Bellevue, Nebraska. Representatives of Cox Communications indicated that the IP address was assigned to the Defendant at a residence in Bellevue, Nebraska. On August 14, 2015, a search warrant was applied for by law enforcement and authorized by the Magistrate Judge, in the District of Nebraska, for the search of the Defendant's residence in Bellevue. Evidence of child pornography was found on computers located at the Defendant's residence.

Defendant has filed a Motion to Suppress all evidence obtained in this case, including evidence obtained from the search warrant applied for in the District of Nebraska on August 21, 2015. In arguing for suppression, the Defendant cites only to the use and deployment of the "network investigative technique" and argues that deployment of the NIT in the Eastern District of Virginia violated Federal Rule of Criminal Procedure 41 and 28 U.S.C. § 636. Defendant does not allege any deficiencies in the application for search warrant obtained in the District of Nebraska, and does not ask for a *Franks* hearing based on any false statements made with respect to either search warrant from the Eastern District of Virginia or from the District of Nebraska.

Defendant's objection relates solely to the search warrant in the Eastern District of Virginia involved in the acquiring of information obtained when the Defendant accessed the Playpen website located in the Eastern District of Virginia.

ARGUMENT

Overview

Defendant argues that the "search" of Defendant's computer was invalid because the magistrate in the Eastern District of Virginia violated Rule 41 of the Federal Rules of Criminal Procedure by issuing a warrant in the Eastern District of Virginia that allowed for the use of the NIT on the Defendant's computer in Nebraska. Defendant asserts that because of this alleged violation of Rule 41, the Defendant was prejudiced and that suppression is the only remedy that can be imposed in this case. Further, Defendant argues that the good-faith exception utilized by the United States Supreme Court in *United States v. Leon*, 468 U.S. 897 (1984), is not applicable in this case because the warrant was invalid. The United States respectfully asserts that Defendant's arguments are without merit and that the Motion to Suppress be denied.

As this Court is uniquely aware, a number of lower courts have addressed the issues posed by the Defendant's Motion to Suppress. See *United States v. Michaud*, 2016WL337263 (W.D. WA 2016); *United States v. Stamper*, 2016WL695,660 (S.D. OH 2016); *United States v. Stamper*, Case No. 1:15CR00109-MRB, Filing 48, (S.D. OH, filed February 19, 2016); *United States v. Epich*, 2016WL953269 (E.D. WI 2016); *United States v. Levin*, 2016WL2596010 (D. MA 2016); *United States v. Arterbury*, 2016 U.S. Dist. LEXIS 67091 (N.D. OK 2016); *United States v. Werdene*, 2016WL3002376 (E.D. PA 2016); *United States v. Matish*, 2016WL3545776 (E.D. VA 2016); and *United States v. Darby*, 2016WL3189703 (E.D. VA 2016). These cases have been copied and are set forth either in the Defendant's Index or in the Government's Index

of Evidentiary materials. In arguing that the Defendant's Motion to Suppress be denied, the United States will address the issues set forth by the Defendant separately,

I. VIOLATION OF RULE 41

Defendant bases his argument on the authority of the magistrate in the Eastern District of Virginia to issue a search warrant which allowed for placing a NIT on a computer located and accessed within the District of Virginia from computers located both within the Eastern District of Virginia and outside that district. In examining the magistrate's powers, the focus and attention is on Rule 41 of the Federal Rules of Criminal Procedure and Title 28, United States Code, Section 636. In pertinent part, Rule 41 of the Federal Rules of Criminal Procedure provide that:

> b) AUTHORITY TO ISSUE A WARRANT. At the request of a federal law enforcement officer or an attorney for the government:
>
> (1) a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property located within the district;
>
> (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;
>
> (3) a magistrate judge—in an investigation of domestic terrorism or international terrorism—with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;
>
> (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and
>
> (5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:

> (A) a United States territory, possession, or commonwealth;
>
> (B) the premises—no matter who owns them—of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or
>
> (C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

Federal Rule of Criminal Procedure 41(b)

Title 28, United States Code, Section 636 states in pertinent part regarding a magistrate judge's duties and jurisdiction:

> (a) Each United States magistrate judge serving under this chapter shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law-
>
> (1) all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure for the United States District Courts . . .

Title 28, United States Code, Section 636(a)

In the case at bar, the FBI did not randomly select individuals to place a NIT on their computers located outside the District of Virginia. In this case, the search warrant was only activated, and the NIT deployed, when a user accessed the Playpen website by typing in a login name and password in to the Playpen website server, at that time located in Virginia. At that point, based on the information contained in the affidavit, there was probable cause to believe that the user was logging in to the website for the purpose of accessing and acquiring child pornography. Only at that time, was the NIT deployed which sought additional information from the user's computer.

At least two cases have determined that the use of the NIT was authorized by Federal Rule of Criminal Procedure 41(b)(4). That rule "endows a magistrate with authority to issue a warrant authorizing the use of a tracking device." *United States v. Matish, supra* at *17. This rule provides that "[t]he tracking device must be installed within the magistrate's district, but the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both." *Id*. quoting Federal Rule of Criminal Procedure 41(b)(4). The district court in *Matish* noted that "whenever someone entered Playpen, he or she made, in computer language, "a virtual trip" via the internet to Virginia, just as a person logging in to a foreign website containing child pornography makes a "virtual trip" overseas." As the court noted, "[b]ecause the NIT enabled the government to determine Playpen user's locations, it resembled a tracking device." *Id*. at *18. The court in *Matish* disagreed with other courts, which held that Rule 41(b)(4) did not apply, noting that "the installation did not occur on the government-controlled computer, but on each computer that entered the Eastern District of Virginia when its user logged in to Playpen via the TOR network. When that computer left Virginia – when the user logged out of Playpen – the NIT worked to determine its location just as traditional tracking devices and foreign law enforcement of a target's location." *Id*.

The reasoning in *Matish* was adopted in *United States v. Darby*, supra at *12. In that case, a separate court in the Eastern District of Virginia found that "nothing in Rule 41 categorically forbids magistrate's from issuing warrants that authorize searches in other districts – most of its provisions do just that." *United States v. Darby*, supra at *11. In *Darby*, the court noted that "Rule 41(b)(4) allows a magistrate to issue a warrant for a tracking device to be installed in the magistrate's district. Once installed, the tracking device may continue to operate even if the object tracked moves outside the district." *Id*. at *12. The *Darby* court noted "[t]his

is exactly analogous to what the NIT warrant authorized. Users of Playpen digitally touched down in the Eastern District of Virginia when they logged in to the site. When they logged in, the government placed code on their home computers. Then their home computers, which may have been outside of the district, sent information to the government about their location. The magistrate judge did not violate Rule 41(b) in issuing the NIT warrant." *Id*.

In the case at bar, the Defendant, through computer directions, accessed a computer located in Virginia. In accessing the Playpen server, the Defendant requested, through computer code, various items from the server, located in Virginia, including images of child pornography. The Defendant requested, through his log-in and password, access to the forums located on the Playpen server, based in Virginia. As the courts in *Matish* and *Darby* note, the Defendant made a "virtual trip" to Virginia in accessing the Playpen website by logging in to the Playpen server. The deployment of the NIT did not occur until the Defendant made the "virtual trip" to Virginia. The magistrate had authority to issue a tracking device on the Defendant's computer when the Defendant's computer makes a "virtual trip" to Virginia. The magistrate had authority under Rule 41 and 28 U.S. § 636. Defendant's Motion to Suppress should be denied.

II. EVEN A TECHNICAL VIOLATION OF RULE 41 DOES NOT WARRANT SUPPRESSION OF THE EVIDENCE

A number of courts addressing suppression issues in cases similar to the one at bar have found that the deployment of the NIT technically violated the letter of Rule 41(b), "but not the spirit of the Rule." *United States v. Stamper*, 1:15-CR-00109, supra, at p.15. Therefore, even if this Court was to find that there was a technical violation of Rule 41(b), suppression of the evidence is still not warranted. Defendant has not established the prerequisites of prejudice or reckless disregard for a provision in the rule to warrant suppression of the evidence. Defendant's Motion should be denied.

"[A]lthough the purpose of Rule 41 is the implementation of the 4th Amendment, the particular procedures it mandates, are not necessarily part of the 4th Amendment." *United States v. Stamper*, *Id.* at p.7, quoting *United States v. Searp*, 586 F.2d 1117, 1121 (6th Cir. 1978), *cert. denied* 440 U.S. 921 (1979). "Even where there is a failure to comply with Rule 41, a search may nevertheless be "reasonable" in the Constitutional sense and meet the requirements of the 4th Amendment." *Id.* "[V]iolations of federal rules do not justify the exclusion of evidence that has been seized on the basis of probable cause, and with advance judicial approval." *United States v. Epich*, supra at *2 (citing *United States v. Cazares-Olivas*, 515 F.3d 726, 730 (7th Cir. 2008).) "Suppression of evidence is rarely, if ever, the remedy for a violation of Rule 41, even if such a violation has occurred." *Id.* (citing *United States v. Berkos*, 543 F.3d 392, 396 (7th Cir. 2008).

"The exclusionary rule is an "instrument" and "[f]or that reason courts should be wary in extending the exclusionary rule in search and seizure cases to violations which are not of constitutional magnitude." *United States v. Hornbeck*, 118 F.3d 615, 618 (8th Cir. 1997), (quoting *United States v. Burke*, 517 F2d 377, 386 (2nd Cir. 1975).) "Indeed, exclusion has always been our last resort, not our first impulse, . . ." *Herring v. United States*, 555 U.S. 135, 140 (2009). "[T]he exclusionary rule is not an individual right and applies only where it "'result[s] in appreciable deterrence.'" *Id.* at 141. The Supreme Court has "repeatedly rejected the argument that exclusion is a necessary consequence of a 4th Amendment violation." *Id.* "[T]o the extent that application of the exclusionary rule could provide some incremental deterrent, that possible benefit must be weighed against [its] substantial social cost." *Id.*, quoting *Illinois v. Krull*, 480 U.S. 340, 352-353 (1987).

A procedural violation is not per se, an unreasonable search and seizure in violation of the 4th Amendment. *United States v. Welch*, 811 F.3d 275, 280 (8th Cir. 2016) (citing *United*

States v. Freeman, 897 F.2d 346, 348-49 (8th Cir. 1990)). Thus, "noncompliance with Rule 41 does not automatically require the exclusion of evidence in a federal prosecution." *United States v. Spencer*, 439 F.3d 905, 913 (8th Cir. 2006) (citing *United States v. Schoenheit*, 856 F.2d 74, 76 (8th Cir. 1988)). Rather, as the Eighth Circuit recently stated, "a Rule 41 violation amounts to a violation of the 4th Amendment warranting exclusion 'only if a defendant is prejudiced or if reckless disregard of proper procedure is evident'". *United States v. Welch*, supra at 279.

"There are two categories of Rule 41 violations: those involving Constitutional violations, and all others." *United States v. Werdene*, supra at p. 6. "Courts have described violations of Rule 41 as either: (1) "substantive" or "Constitutional" violations; or (2) "ministerial" or "procedural" violations." *Id.* There is no question that the majority of courts considering the NIT warrant related to the "Playpen" TOR-network-based child pornography investigation have found no Constitutional violation occurred even where the court found that the issuance of a NIT warrant technically violated Rule 41. *See United States v. Michaud*, supra at *6-7; *United States v. Werdene*, supra at p. 8-9; *United States v. Matish*, supra at p. 25-27; and *United States v. Darby*, supra at p.14. Defendant essentially argues that the alleged violation of Rule 41 is a substantive violation because the court lacked authority to issue the warrant. However, "[t]o demonstrate that the violation of Rule 41 was of Constitutional magnitude, [the defendant] must show a violation of his 4th Amendment rights." *United States v. Werdene*, supra at p.6. "Specifically, he must articulate how the government's failure to comply with Rule 41(b) caused a search or seizure prohibited by the 4th Amendment. He cannot do so." *Id.*

In the case at bar, Defendant cannot articulate how the government's alleged failure to comply caused a search or seizure prohibited by the 4th Amendment. First, the issuance of the NIT warrant clearly complied with the 4th Amendment. The 4th Amendment demands three

things from a search warrant. A warrant must be issued by a neutral magistrate; and must be based on a showing of "probable cause to believe that the evidence sought will aid in a particular apprehension or conviction for a particular offense"; and it must satisfy the particularity requirement. See *United States v. Dahlia*, 441 U.S. 238, 255 (1978). Defendant does not argue that the warrant was not issued by a neutral and detached magistrate, lacked probable cause, or failed to satisfy the particularity requirement. In essence, Defendant argues, as *Werdene* argued, the circular argument that government's alleged "violation of Rule 41 is of Constitutional magnitude because it did not involve mere ministerial violations of the rule." *United State v. Werdene*, supra at p. 6. That is insufficient to establish a Constitutional violation. The warrant authorized by the magistrate of the Eastern District of Virginia clearly met all of the qualifications of a proper warrant and Defendant's argument should fail. Further, there was jurisdiction to authorize the warrant in the Eastern District of Virginia. That was where the server that was being accessed was located. That was the most logical location to acquire a warrant. Contrary to the decisions in *Levin* and *Arterbury*, the warrant here was not void *ab initio*, as if there was no warrant at all. The magistrate clearly did have authority to issue the warrant in the Eastern District of Virginia. There is no constitutional violation in this case.

Moreover, the application of the 4th Amendment "depends on whether the person invoking its protections can claim a 'justifiable,' or 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by the government action." *Id.* at p. 6, quoting *Smith v. Maryland*, 442 U.S. 735, 740 (1979). In the above-captioned matter, the Defendant had no expectation of privacy in the information being requested through the deployment of the NIT. An individual has "no reasonable expectation of privacy in his IP address and so cannot establish a 4th Amendment violation." *United States v. Werdene*, supra at p.7, quoting *United States v.*

Christie, 624 F.3d 547 (3rd Cir. 2010). "No reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and, indeed from third parties including [internet service providers]." *Id. See also, United States v. Matish* supra at p. 26. ("Generally, no one has reasonable expectation of privacy in an IP address when using the internet."); *United States v. Wheelock*, 772 F.3d 825, 828 (8th Cir. 2014); (". . . Wheelock cannot claim a reasonable 'expectation of privacy in [the] government's acquisition of his subscriber information, including his IP address and name from third party service providers.'"); and *United States v. Perrine*, 518 F.3d 1196, 1204-05 (10th Cir. 2008) (every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the 4th Amendment privacy expectation.").

Defendant's argument of a substantive or Constitutional violation is simply without merit. At best, any alleged violation that occurred in this case was a technical violation of Rule 41, as determined by the majority of the courts. Defendant's arguments of a substantive violation should be denied.

III. EFFECT OF TECHNICAL VIOLATION OF RULE 41 ON SUPPRESSION OF EVIDENCE

As no Constitutional violation can be established by Defendant, any alleged Rule 41(b) violation should be considered a "technical violation" of that rule. As such, "where a technical Rule 41(b) violation occurs, courts may suppress where a defendant suffers prejudice, in the sense that the search would not have occurred . . . if the rule had been followed, or where law enforcement intentionally and deliberately disregarded the rule." *United States v. Michaud*, supra at p. 6, (quoting *United States v. Weiland*, 420 F.3d 1062, 1071 (9th Cir. 2005). In the case at bar, the Defendant cannot establish prejudice or an intentional or deliberate disregard for Rule 41. Defendant's Motion to Suppress should be denied.

Similar arguments have been rejected in other courts. In *Werdene*, the district court determined that *Werdene's* did not establish prejudice as defined by Third Circuit case law. The Third Circuit defines prejudice "in the sense that it offends concepts of fundamental fairness or due process." *United States v. Werdene*, supra at p. 8. After stating this legal standard, the court determined that *Werdene* was not prejudiced by the officer's actions. The court noted that:

> After assuming control of Playpen and moving the server to a government facility in Newington, Virginia, Agent MacFarland sought and obtained a warrant to employ the NIT in the Eastern District of Virginia [citation omitted] before activating the NIT, Agent MacFarland did not – and could not – know that Werdine resided in the Eastern District of Pennsylvania. Indeed, the only way the government could have procedurally complied with Rule 41, was either through sheer luck (i.e., Werdene's location happened to be within the Eastern District of Virginia) or by applying for a warrant in everyone one of the 94 federal judicial districts. Agent MacFarland's warrant application, which was approved by a neutral and detached magistrate, described the NIT process in copious detail. [Citation omitted]. The warrant application states that the NIT was deployed "each time that any user or administrator log[ged] into Playpen by entering a username and password." [Citation omitted] This enabled the FBI to link a username and its corresponding activity to an IP address. [Citation omitted] Agent MacFarland specifically noted that the NIT could enable this process on users of Playpen "wherever located." [Citation omitted] The government's non-Constitutional violation of Rule 41 does not offend concepts of fundamental fairness or due process and Werdine's Motion to Suppress cannot be granted on prejudice grounds."

United States v. Werdene, supra at p. 8-9.

A similar argument was rejected in *United States v. Michaud*, 2016WL337263 (W.D. WA. 2016). The defendant in *Michaud* used similar arguments to the Defendant in the case at bar. The court in *Michaud* rejected these arguments.

> First, considering the prejudice, [defendant] would have the court interpret the definition of prejudice found in *Weiland* and elsewhere, "in the sense that the search would not have occurred . . . if the rule had been followed." to mean that the defendant suffers prejudice whenever a search occurs that violates Rule 41(b). This interpretation makes no sense, because under that interpretation all searches executed on the basis of warrants in violation of Rule 41(b) would result in prejudice, no matter how small or technical the error might be. Such an interpretation would defeat the need to analyze prejudice separately from the Rule

> 41(b) violation. Tracing the origin of the definition used in *Weiland* to its early use in the Ninth Circuit yields a more sensible interpretation of the well-established definition: "In the sense that the search would not have occurred . . . if the rule had been followed" suggests that courts should consider whether the evidence obtained from a warrant that violates Rule 41(b) could have been available by other lawful means, and if so, the defendant did not suffer prejudice. See *United States v. Vasser*, 648 F.2d 507, 511 (9th Cir. 1980).

United States v. Michaud, supra at p. 6.

In applying the standard for prejudice, the court in *Michaud* rejected the Defendant's arguments. The court noted:

> Applying that interpretation here, [defendant] did not suffer prejudice. [Defendant] has no reasonable expectation of privacy of the most significant information gathered by deployment of the NIT, [defendant's] assigned IP address, which ultimately led to [defendant's] geographic location. [Citation omitted] Although the IP addresses of users utilizing the TOR network may not be known to websites, like Website A, using the TOR network does not strip users of all anonymity, because users accessing Website A must still send and receive information, including IP addresses, through another computer, such as an internet service provider, at a specific physical location. Even though difficult for the government to secure that information tying the IP address to [defendant], the IP address was public information, like an unlisted telephone number, and eventually could have been discovered.

United v. Michaud, supra at p. 6.

This analysis was also adopted by the Southern District of Ohio in *United States v. Stamper*, 1:15CR00109, Filing 48 (S.D. OH 2016). In rejecting defendant's argument that he was prejudiced by the government's actions, the district court noted that "defendant argues that based on these statements, the search of his computer would not have occurred if Rule 41(b) had been followed. The court disagrees. The information seized by the NIT did not lead to defendant directly. Instead, the FBI agents only learned defendant's IP address as a result of the NIT warrant. Defendant did not suffer prejudice by having this information revealed. The court agrees with the court in *Michaud* on this point . . ." *United States v. Stamper*, 1:15CR00109, Filing 48, p. 21-22 (S.D. OH 2016).

Defendant does not identify how he was prejudiced by the issuance of the NIT warrant. To the extent there was prejudice, it was caused by the Defendant's actions in accessing the Playpen website and logging in and using a username and password. The use of the TOR network made his IP address harder to determine, but the Defendant's IP address was still public information. His IP address had been provided to a third party, whether an internet service provider or a server on the TOR network. Even if Rule 41 authorized the NIT to be deployed to users in the Eastern District of Virginia, that information would not be known until after the Defendant logged in to the Playpen website and the NIT was deployed. In other words, the information would have been obtained even if the rule had been followed. Defendant's arguments that the warrant should have been issued by a judge within the District of Nebraska is equally without merit. There is no indication, based upon the warrant's compliance with the 4th Amendment that it could not have, or would not have been issued here. Clearly probable cause existed in the District of Nebraska. Indeed, had Defendant not attempted to conceal his true location, the government could have obtained the search warrant from the magistrate in this district. Such an argument does not support a claim of prejudice that should result in suppression. The Ninth Circuit, for instance, has found no prejudice to exist from a Rule 41 violation where "circumstances under which the warrant was sought at least partially justified the agent's deviation from the letter of the rule" and a warrant "complies with the spirit of Rule 41 in that it provided a basis for a probable cause determination and established an adequate record to review that determination." *United States v. Vassar*, supra at p. 510. Moreover, "[t]he policies behind the exclusionary rule are not absolute and must be evaluated realistically and pragmatically on a case by case basis." *Id.* Nor should this Court, "fault the good-faith ingenuity of the officers" in responding to the Defendant's use of advanced technology with its

own, where "interest protected by the 4th Amendment and Rule 41 were safeguarded by the officers . . . even though the methods used were novel." *Id.* As the court noted in *Michaud*, [Rule 41] does not directly address the kind of situation that the NIT warrant was authorized to investigate, namely where criminal suspects geographical whereabouts are unknown, perhaps be design, but the criminal suspects have made contact via technology with the FBI in a known location." *United States v. Michaud*, supra at *6. Defendant's argument of prejudice is misplaced and should be rejected by this Court.

IV. INTENTIONAL AND DELIBERATE DISREGARD OF RULE 41(B).

Although Defendant does not specifically argue that FBI agents engaged in intentional and deliberate disregard of Rule 41(b), it is clear from the record that agents did not intentionally or deliberately disregard Federal Rule of Criminal Procedure 41(b). Therefore, even if the government technically violated Rule 41(b), suppression is not warranted.

As the court held in *Werdene*, a review of the record, including the warrant application from the Eastern District of Virginia, "shows no deception on the government's part. The warrant request was candid about the challenge that the TOR network poses, specifically its ability to mask a user's physical location.[‘] Agent MacFarland stated that the NIT would be deployed "each time" that "any user" logged in to Playpen "wherever" they were "located." [Citation omitted] . . . [T]he government did not mislead the magistrate judge but instead was up front about the NIT's method and scope." *United States v. Werdene*, supra at p. 9. The holding in *Werdene* has been supported by the majority of cases which have analyzed this issue. See *United States v. Matish*, supra at *24, p. 31 ("additionally, defendant failed to show an intentional or deliberate disregard of Rule 41(b)."); *United States v. Michaud*, supra at *7, p. 6 ("[Defendant] also fails to show that the FBI acted intentionally and with deliberate disregard of

Rule 41(b)."); and *United States v. Stamper*, Case 1:15CR00109, Filing 48, p. 22-23 ("Next the court finds that there is no evidence of intentional and deliberate disregard of Rule 41(b). The government specifically requested a search warrant authorizing that "the NIT may cause an activating computer – *wherever located* – to send to a computer controlled by or known to the government, network level messages containing information that may assist in identifying the computer, it's location, other information about the computer and the user of the computer, as described above and in Attachment B."). There is clearly no evidence of an intentional or deliberate disregard of Rule 41 in the application for search warrant in the Eastern District of Virginia.

V. *LEON* GOOD-FAITH EXCEPTION APPLIES IN THIS CASE.

Defendant argues that because the warrant was allegedly void at the outset, officers did not have good-faith to execute the warrant duly signed by the magistrate judge in the Eastern District of Virginia. Moreover, although not expressly argued in this case, Defendant's argument appears to be that the investigating officer in the District of Nebraska did not have good-faith in relying upon the information provided by FBI agents based upon the allegedly illegal warrant in the Eastern District of Virginia. In this case, a magistrate in Nebraska was specifically told all of the facts related to the collection of data that demonstrated probable cause for a search warrant to be executed in the District of Nebraska. The Nebraska magistrate, given all of those facts, signed a warrant for the search of the Defendant's residence. There is no argument by the Defendant that the agent in Nebraska lied or mislead the Nebraska magistrate. The Nebraska agent duly executed the search warrant signed by the Nebraska magistrate. Defendant's argument that the good-faith exception does not exist in this case is clearly erroneous and should be rejected by this Court.

"When the government seeks to admit evidence collected pursuant to an illegal search or seizure, the exclusionary rule operates to suppress that evidence and makes it unavailable at trial." *United States v. Werdene*, supra at p. 9. "The exclusionary rule was developed "[t]o deter 4th Amendment violations." " *Id.* "Where a warrant is executed in good faith, even if the warrant itself is subsequently invalidated, evidence obtained need not be suppressed." *United States v. Michaud*, supra at *7, citing *United States v. Leon*, 468 U.S. 897, 922 (1984). "Warrants may be invalidated for technical or fundamental (constitutional) violations [Citations omitted]." *Id.* "Whether a warrant is issued in good faith depends upon whether reliance on the warrant was objectively reasonable." *Id.*, citing *United States v. Leon*, supra at 922. "Whether suppression is appropriate under the exclusionary rule is a separate question from whether a defendant's 4th Amendment rights were violated." *United States v. Werdene*, supra at p. 9. "The fact that a 4th Amendment violation occurs does not mean that the evidence is automatically suppressed." *Id.*, citing *United States v. Katzin*, 769 F.3d 163, 170 (3rd Cir. 2014) (en banc) cert. denied 135 S. Ct. 1448 (2015). "Indeed, exclusion 'has always been our last resort, not our first impulse.'" *Id.*, quoting *Herring v. United States*, 555 U.S. 135, 140 (2009).

With respect to both the warrant obtained in the Eastern District of Virginia, and the warrant obtained in the District of Nebraska, officers acted in good faith reliance upon the magistrate's execution of the search warrants in question. "When police act under a warrant that is invalid for a lack of probable cause, the exclusionary rule does not apply if the police acted 'in an objectively reasonable reliance' on the subsequently invalided search warrant." *United States v. Darby*, supra at *13, p.15. , quoting *United States v. Leon*, 468 U.S. 897, 922 (1984). "Searches pursuant to a warrant will rarely require any deep inquiry into reasonableness." *United States v. Michaud*, supra at *7, p. 7, quoting *United States v. Leon*, 468 U.S. at 922. As

the vast majority of cases noted, the officers in the Eastern District of Virginia were clearly reasonable in obtaining and executing a search warrant in the Eastern District of Virginia. The court in *United States v. Werdene* gave a detailed description of the agent's objective reasonableness in applying for an executing the warrant in the Eastern District of Virginia. The court noted that "[t]he agents in this case acted upon a reasonably objective good faith belief in the legality of their conduct." *United States v. Werdene*, supra at p.11. As the court notes in *Werdene*, both the attachments to the search warrant and the affidavit clearly define the scope and breadth of the warrant being applied for by the agents. Because of this, an "objectively reasonable" reading of the warrant gave the agents "authority to deploy the NIT from a government-controlled computer in the Eastern District of Virginia against anyone logging on to Website A, with any information gathered by the NIT to be returned to the government-controlled computer in the Eastern District of Virginia." *United States v. Werdene*, supra at p. 11-12, quoting *United States v. Michaud*, supra at *4. The court in *Werdene* further noted that "[c]ontrary to [defendant's] assertion, this is not a case where the agents "hid the ball" from the magistrate or misrepresented how the search would be conducted." *Id*. at p. 12. As the court noted in *Darby*:

> "The FBI agents in this case did the right thing. They gathered evidence over an extended period and filed a detailed affidavit with a federal magistrate in support of their search warrant application. They filed the warrant application in the federal district that had the closest connection to the search to be executed. The information gathered by the warrant was limited; primarily the IP addresses of those that accessed Playpen and additional information which would aid in identifying what computer accessed the site and which individual used that computer . . . "
>
> "In short, the officers in charge of this investigation are not culpable at all. Additionally, as discussed above, there is no evidence that any failure by the FBI to understand the intricacies of the jurisdiction of federal magistrates was deliberate. Even if the NIT warrant was void because not authorized by the federal magistrate's act, suppression is not warranted in this case."

United States v. Darby, supra at *13-14, p. 15.

The same analysis can apply with even greater force to the search warrant obtained within the District of Nebraska. Here, the agent relied upon information provided by FBI from the Eastern District of Virginia. The agent in Nebraska clearly delineated the facts to the United States federal magistrate judge and requested a warrant to search the Defendant's home. There is no allegation that the agent in Nebraska, either deliberately or with intentional disregard for the truth, misstated the facts contained in the application and affidavit for search warrant. The Nebraska magistrate, duly authorized to issue a search warrant in the District of Nebraska, authorized the search of the Defendant's home. There is no basis from which to find that the Nebraska agent failed to act in good faith in executing the search of the Nebraska residence of the Defendant. The good faith argument adopted by the majority of cases looking at the Playpen search warrant would apply with even greater force to the evidence obtained at the Defendant's residence in Nebraska pursuant to the Nebraska search warrant.

The crux of Defendant's argument is that because the warrant was allegedly void at the outset, there could have been no jurisdiction to issue the warrant. Therefore, law enforcement officers did not have reasonably good faith in executing the allegedly void warrant. This argument was completely rejected by the court in *Werdene.* As the *Werdene* court notes, defendant's argument was adopted by the District Court of Massachusetts in *United States v. Levin* and agreed with in *Aterbury*. The court in *Werdene* forcefully deconstructs the argument set forth in *Levin* and disagrees with its application. As the court in *Werdene* notes, *Levin's* primary reliance on the Sixth Circuit case of *United States v. Scott*, 260 F.3d 512 (6th Cir. 2001), is misplaced, "particularly given the court's acknowledgement that the "Sixth Circuit effectively reversed [*Scott*]" in *United States v. Master*, 614 F.3dd 236 (6th Cir. 2011)". *United States v.*

Werdene, supra at *10. In rejecting the argument set forth in *Levin*, the court in *Werdene*, analyzed the United States Supreme Court opinion in *Herring v. United States*, supra, and found that "[t]he good-faith exception is not foreclosed in the context of a warrant that is void *ab initio* and the court must now determine if [the good-faith exception] applies."

It is clear that the status of the warrant as being "void" is separate from the application of the good-faith exception under *Leon*. "In other words, the legal status of the warrant under the 4th Amendment does not inform the decision of whether the good-faith exception is available in a given case; that inquiry is separate and must be considered in light of the exclusion rule's purpose and the officer's conduct at issue." See *United States v. Werdene*, supra at p.11, quoting *United States v. Master*, 614 F.3d at 243. Other courts have refused to suppress evidence obtained from warrants that were later found invalid, due to the judge's lack of authority. See, e.g., *United States v. Master*, 614 F.3d at 242-243; *United States v. Hernandez*, 2008WL4748576, *16-17 (D. MINN. October 28, 2008) (denying motion to suppress where a search warrant was issued by a unauthorized judge in violation of Rule 41, where there was "no evidence that the search warrant would not have been issued otherwise."); *United States v. Mann*, 2007WL4321969, *23 (D.MINN. December 6, 2007); and *United States v. LaFountain*, 252 F.Supp.2d 883, 891 (D. MD. 2003).

Defendant's argument is also inconsistent with Supreme Court case law. The Supreme Court has made clear that "suppression is not an automatic consequence of a 4th Amendment violation," but instead "turns on the culpability of the police and the potential of exclusion to deter wrongful police conduct." *Herring v. United States*, supra at 137; *Illinois v. Gates*, 462 U.S. 213, 223 (1983) ("the fact that a 4th Amendment violation occurred – i.e., that a search or arrest was unreasonable – does not necessarily mean that the exclusionary rule applies."). In

Herring, the Supreme Court refused to suppress evidence obtained from the warrantless search of the defendant's person and vehicle incident to his arrest pursuant to a non-existent arrest warrant. See Herring v. United States, supra at 147. The Court explained that, "[t]o trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficient culpable that such deterrence is worth the price paid by the justice system." *Id* at 144. *Herring* makes clear that the good-faith exception applies to a search conducted pursuant to a warrant that is void from the outset. That case involving the arrest of an individual pursuant to a warrant that had been rescinded five months earlier. (H*erring v. United States*, supra at p. 137-138.) Although the arrest warrant had no legal force – since it no longer existed – and thus did not authorize the defendant's arrest, the Supreme Court proceeded to consider whether the officer's reliance on the invalid warrant was objectively reasonable in determining whether evidence obtained from the warrant and search incident to the unlawful arrest should be suppressed.

Therefore, in the case at bar, even if this Court were to find that the NIT warrant, like the arrest warrant in *Herring*, was no warrant at all, *Herring* dictates that suppression is not automatic, and that the officer's good faith – as well as the deterrent benefits of suppression – must be considered in deciding whether to invoke the exclusionary rule. As already stated, cases have clearly found that the officers were objectively reasonable in conducting searches as directed by the magistrate judge in the Eastern District of Virginia. Furthermore, in the immediate case at bar, the Nebraska law enforcement agents were objectively reasonable in relying upon the search warrant obtained by the magistrate in the District of Nebraska for the search of the Defendant's residence in Nebraska. Defendant's argument that the good-faith exception does not apply is simply without merit.

Finally, the court in both *Levine* and *Arterbury* failed to use the balancing test for suppression of the evidence outlined in *Leon* and *Herring*. As the Supreme Court has emphasized, "[e]ach time the exclusionary rule is applied it exacts a substantial social cost for the vindication of 4th Amendment rights." *United States v. Darby*, supra at *13, p. 15, quoting *Rakas v. Illinois*, 439 U.S. 128 (1978). "The exclusionary rule should only be applied when its benefits outweigh its costs." *Id.* quoting *Herring v. United States*, 555 U.S. at 41. As the court in *Werdene* noted, "the court in *Levin* did not analyze the "cost" associated with suppression." *United States v. Werdene*, supra at p. 12. The court in *Werdene* also noted that "[t]he court in *Levin* also did not address what deterrent effect, if any, suppression would have in this case. While the court found that the agent's conduct constituted "systemic error or [a] reckless disregard of Constitutional requirements" it failed to address why that is the case." *Id.* "*Levin* seemed to overlook the Supreme Court's directive that "the exclusionary rule is not an individual right and applies only where it result[s] in appreciable deterrence." *Id.*, quoting *United States v. Herring*, 555 U.S. at 141. As the court found in *Werdene*, "to the extent a mistake was made in this case, it was not made by the agents and "reckless . . . disregard for 4th Amendment rights." [citation omitted], "rather it was made by the magistrate when she mistakenly issued a warrant outside her jurisdiction." *Id.* The agent's "presented the magistrate judge with all relevant information to allow her to make a decision as to whether Rule 41(b) permitted her to issue the warrant. The FBI agents did not misrepresent how the search would be conducted or, most importantly, where it would be conducted . . . a magistrate's mistaken belief that she had jurisdiction, absent any initia of reckless conduct by the agents, does not warrant suppression." *Id.* "Exclusion of the evidence in this case would only serve to "punish the error of judges and magistrates" and would not have any "appreciable" effect on law enforcement." *Id.* at p. 12-13,

quoting *United States v. Leon*, 468 U.S. at 909, 916. "Once the warrant was issued, albeit outside the technical bounds of Rule 41(b), the agents acted upon an objectively reasonable belief in the legality of their conduct." *United States v. Werdene*, supra at p. 13. See also, *United States v. Leon*, supra at 921 ("in the ordinary case, an officer cannot be expected to question the magistrate's . . . judgment that the form of the warrant is technically sufficient . . . penalizing the officer for the magistrate's error, rather than his own, cannot logically contribute to the deterrence of 4th Amendment violations."). As in the case at bar, the court in *Werdene* found "[t]he "cost" of suppression, therefore, would be letting "a guilty and possibly dangerous defendant[] go free – something that 'offends basic concepts of the criminal justice system.'" *Id.*, quoting *Herring v. United States*, 555 U.S. at 141. "Absent any appreciable deterrent effect on law enforcement, suppression would only serve to "exact[]" a heavy toll on both the judicial system and society at large." *Id.*

The cost of suppression would be even greater in the case at bar. In this case, agents provided the magistrate in Nebraska a clear and complete recitation of the facts supporting probable cause for a search of the Defendant's residence. The magistrate judge, after reviewing the affidavit and application for search warrant, concluded that probable cause existed for a search of the Defendant's residence. Agents properly relied on that search warrant and executed the warrant at the Defendant's residence, finding evidence that the Defendant was receiving and possessing child pornography. Clearly the cost of suppression in this case outweigh any deterrent effect on law enforcement officers who properly go before magistrates in order to obtain search warrants. As the court noted in *Darby*, the agents in this case did the right thing. Suppression is not warranted in this case.

CONCLUSION

For the reasons stated herein, the United States respectfully requests this Court to enter an order denying the Defendant's Motion to Suppress.

Respectfully submitted,

DEBORAH R. GILG
United States Attorney
District of Nebraska

By: s/ Steven A. Russell
STEVEN A. RUSSELL, #16925
Assistant U.S. Attorney
100 Centennial Mall North
487 Federal Building
Lincoln, NE 68508-3865
Tel: (402) 437-5241
Fax: (402) 437-5390
E-mail: steve.russell@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on July 11, 2016, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which sent notification of such filing to the following: Jim McGough, Esq, and also hereby certify that a copy of the same has been served by regular mail, postage prepaid, to the following non-CM/ECF participants: N/A.

s/ Steven A. Russell
Assistant U.S. Attorney